

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

BEVERLY T PETERS,

Plaintiff,

VS.

ST. JOSEPH SERVICES CORPORATION
d/b/a ST. JOSEPH HEALTH SYSTEM, *et al*,

Defendants.

§
§
§
§
§
§
§
§

CIVIL ACTION NO. 4:14-CV-2872

MEMORANDUM OPINION AND ORDER

I. INTRODUCTION

The plaintiff, Beverly T. Peters (“Peters”), brings this class action lawsuit against the defendants, St. Joseph Services Corporation d/b/a St. Joseph Health System, and St. Joseph Regional Health Center (collectively, “St. Joseph”), for damages arising from an intrusion into St. Joseph’s computer network and the resulting data breach. Peters alleges violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (“FCRA”), and various state and common law claims sounding in tort and contract. Pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure, St. Joseph moves to dismiss the First Amended Class Action Complaint (the “Complaint”) for lack of standing and, alternatively, for failure to state a claim under Rule 12(b)(6) (Doc. Entry Nos. 26 & 27). St. Joseph has also filed motions to strike and to deny class certification (Doc. Entry Nos. 24 & 25).

This case raises an issue of first impression in this Circuit: whether the heightened risk of future identity theft/fraud posed by a data security breach confers Article III standing on persons whose information may have been accessed.¹ Having reviewed the parties’ submissions and the

¹ The issue was presented to the Texas Court of Appeals in *Bliss & Glennon, Inc. v. Ashley*, 420 S.W.3d 379 (Tex. App.—Houston [1st Dist.] 2014), on review of a denial to dismiss the defendant’s counterclaims. The court avoided

relevant law, the Court concludes that the answer is no. Based on this determination, the Court finds that Peters has not alleged cognizable Article III injury and therefore lacks standing to bring her federal claims. The Court GRANTS St. Joseph's Rule 12(b)(1) motion to dismiss (Doc. Entry No. 26) and does not reach the merits of the remaining motions.²

II. FACTUAL BACKGROUND

St. Joseph is a health care service provider headquartered in Texas. Peters, a resident of Texas and a former St. Joseph patient, gave her personally identifiable information and/or protected health information (collectively, "personal information") to St. Joseph during the course of purchasing health care services from it. The information, stored on the St. Joseph computer network, included her name, social security number, birthdate, address, medical records and bank account information.

In a letter on February 4, 2014, St. Joseph announced that between December 16, 2013 and December 18, 2013, a security breach of its computer system occurred (the "Data Breach"). It was reported that hackers had infiltrated its computer network and potentially gained access to the personal information of Peters and approximately 405,000 other "[St. Joseph] patients, employees, and some employees' beneficiaries" (the "Class Members").³ Upon discovery of the attack on December 18, 2013, St. Joseph shut down access to the involved computer.

the constitutional question—i.e., whether the defendant's fear of future identity fraud was a cognizable Article III injury—however, noting that the issue is "far from settled under federal law." *Id.* at 390. The court held that the defendant had standing because the counterclaims contained plausible allegations that his personal data was actually misused. *Id.* at 390□91.

² The Court expresses no opinion as to the viability of Peters' claims under Rule 12(b)(6) since its 12(b)(1) ruling is dispositive. See *Ramming v. United States*, 281 F.3d 158, 161 (5th Cir. 2001) (citing *Hitt v. City of Pasadena*, 561 F.2d 606, 608 (5th Cir. 1977) ("[W]here both [12(b)(1) and 12(b)(6)] grounds for dismissal apply, the court should dismiss only on the jurisdictional ground . . . without reaching the question of failure to state a claim . . .")).

³ Peters defines the Class Members as follows:

St. Joseph further reported that although it was not aware that any personal information had been misused, it made arrangements to provide potentially affected persons one year of free credit monitoring and identity theft protection. Enrollment in the service was automatic, requiring no action by Peters or the Class Members, and made effective as of the date of the letter. St. Joseph encouraged Peters and the Class Members to take steps to safeguard their personal information by monitoring their credit reports and account statements.

In her 13-count Complaint, Peters alleges that during the Data Breach, the hackers accessed and stole her information from the St. Joseph network, then disseminated it into the public domain where it has been misused by unauthorized and unknown third parties. On one occasion, someone attempted to make a retail purchase on her Discover card, which she previously submitted to St. Joseph in connection with purchasing health care services. Upon receiving a fraud alert from Discover, Peters declined approval for the transaction. The company then closed her account and reissued a new payment card to her. Peters was never charged for the attempted purchase.

It is alleged that on another occasion, someone attempted to access Peters' Amazon.com account by using her son's name. Peters claims that the name could only have been obtained from names and next-of-kin information she provided to St. Joseph before the Data Breach. Peters asserts that the Data Breach is also the reason that she receives daily telephone solicitations from medical products and services companies. The callers, she alleges, ask to speak with specific family members, whose contact information is recorded in her personal information.

All Texas residents who were sent a letter or other communication by St. Joseph notifying them that their personally identifiable information and/or protected health information was maintained on a St. Joseph Health System computer system server that was breached by hackers between December 16, 2013 and December 18, 2013, inclusive.

Peters further complains that as a result of the Data Breach, her email account and mailing address were compromised. Her friends and relatives have received large volumes of spam email from her account and she, herself, has received unsolicited marketing materials and emails targeting the medical conditions recorded in her personal information.

Peters broadly asserts, based on information gleaned from the United States Government Accountability Office (“GAO”) and the Federal Trade Commission (“FTC”), that she and the Class Members are now vulnerable to future attacks by thieves who may seek to commit any number of identity theft-related crimes.

III. CONTENTIONS OF THE PARTIES

St. Joseph moves to dismiss the Complaint, contending that the Court lacks subject matter jurisdiction to hear Peters’ claims because she has not suffered an injury, actual or imminent, that is traceable to St. Joseph’s conduct. Regarding actual injury, St. Joseph argues that Peters has not alleged any unreimbursed cost, damage or loss that is causally connected to the theft/fraud that she alleges. Regarding threatened injury, St. Joseph contends that Peters’ claim that she and the Class Members face an elevated risk of future identity theft/fraud that is not “imminent” within the meaning of well-established standing principles. Applying *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013), *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), *cert. denied* 132 S. Ct. 2395 (2012), and *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013), St. Joseph urges the Court to reject the invitation to relax these principles in data breach cases.

Peters contends that St. Joseph’s approach is ill-suited for analyzing standing where, like here, a data breach has given rise to specific incidents of identity theft/fraud and has “increased the risk of additional real and impending” theft/fraud. As briefed, Peters’ Article III analysis in

part turns on the ability of the FCRA to confer standing, based on a private right of action under its provisions.⁴ Her analysis also turns on the holdings in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), and *Pisciotta v. Old Nat. Bancorp.*, 499 F.3d 629 (7th Cir. 2007), which she cites in support of her theory of cognizable future harm. She further relies on district court rulings since *Clapper* that have recognized Article III standing for claims of future harm suffered by data breach victims. See *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp.2d 942 (S.D. Cal. 2014); *Moyer v. Michaels Stores*, No. 14-C-561, 2014 WL 3511500 (N.D. Ill. Jul. 14, 2014); *In re Zappos.com, Inc.*, MDL No. 2357, 2013 WL 4830497 (D. Nev. Sept. 9, 2013).

IV. STANDARD OF REVIEW

Federal courts are courts of limited jurisdiction, and must dismiss a case if, “at any time,” it is determined that subject matter jurisdiction is lacking. FED. R. CIV. P. 12(b)(1), 12(h)(3); see *Stockman v. Fed. Election Comm’n*, 138 F.3d 144, 151 (5th Cir. 1998). “A case is properly dismissed for lack of subject matter jurisdiction when [a federal] court lacks the statutory or constitutional power to adjudicate the case.” *Home Builders Ass’n of Miss., Inc. v. City of Madison*, 143 F.3d 1006, 1010 (5th Cir. 1998) (quoting *Nowak v. Ironworkers Local 6 Pension Fund*, 81 F.3d 1182, 1187 (2d Cir. 1996)). The party seeking to invoke the jurisdiction of a federal court carries “the burden of proving subject matter jurisdiction by a preponderance of the evidence.” *Vantage Trailers, Inc. v. Beall Corp.*, 567 F.3d 745, 748 (5th Cir. 2009) (citing *New Orleans & Gulf Coast Ry. Co. v. Barrois*, 533 F.3d 321, 327 (5th Cir. 2008)).

⁴ The argument conflates Article III standing and statutory standing, which are separate and distinct jurisdictional issues. The Article III question asks whether a party has brought a claim—*any* claim, statutory or otherwise—that the Constitution recognizes. As discussed below, the injury must satisfy Article III’s “case or controversy” requirement. The statutory question, by contrast, asks whether a party has the right to sue under a specific statute. The injury must satisfy the statute’s requirements for bringing a cause of action. Article III standing is mandatory for every claim, and therefore an antecedent inquiry to any claim of statutory standing.

When evaluating jurisdiction, “a [federal] court is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case.” *MDPhysicians & Assoc., Inc. v. State Bd. of Ins.*, 957 F.2d 178, 181 (5th Cir. 1992) (citing *Williamson v. Tucker*, 645 F.2d 404, 413 (5th Cir. 1981)); see *Vantage Trailers*, 567 F.3d at 748 (reasoning that “[i]n evaluating jurisdiction, the district court must resolve disputed facts without giving a presumption of truthfulness to the plaintiff’s allegations”). In making its ruling, the court may rely on any of the following: “(1) the complaint alone, (2) the complaint supplemented by undisputed facts evidenced in the record, or (3) the complaint supplemented by undisputed facts plus the court’s resolution of disputed facts.” *MDPhysicians*, 957 F.2d at 181 n.2 (citing *Williamson*, 645 F.2d at 413).

V. ANALYSIS AND DISCUSSION

Because the parties are non-diverse, subject matter jurisdiction turns on the viability of the federal claims raised in this suit. These claims appear in counts 1 and 2 of the Complaint. The Court must first determine whether Article III standing exists with respect to these claims before reaching the remaining state and common law claims, which fall within the Court’s supplemental jurisdiction. *Cf. DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (noting that Article III standing must exist for each claim alleged and each form of relief sought).

In counts 1 and 2, Peters alleges willful and negligent violations of the FCRA. The FCRA imposes restrictions on any person, as that term is defined by the statute, who “regularly . . . assembl[es] or evaluat[es] consumer credit information . . . for the purpose of furnishing consumer reports to third parties.” 15 U.S.C. § 1681 a(b), (f). Any person who willfully or negligently “fails to comply with any requirement imposed under [the FCRA] with respect to any consumer is liable to that consumer.” *Id.* §§ 1681n(a); 1681o. Peters alleges that St. Joseph

violated the following FCRA provisions: 15 U.S.C. § 1681(b),⁵ 15 U.S.C. § 1681a(d)(3),⁶ 15 U.S.C. § 1681b(a) and (g),⁷ and/or 15 U.S.C. § 1681c(a)(6).⁸ She claims that but for St. Joseph's

⁵ 15 U.S.C. § 1681(b) states:

(b) Reasonable procedures

It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

⁶ 15 U.S.C. § 1681a(d)(3) states:

(3) Restriction on sharing of medical information

Except for information or any communication of information disclosed as provided in section 1681b(g)(3) of this title, the exclusions in paragraph (2) [narrowing definition of "consumer report"] shall not apply with respect to information disclosed to any person related by common ownership or affiliated by corporate control, if the information is—

(A) medical information;

(B) an individualized list or description based on the payment transactions of the consumer for medical products or services; or

(C) an aggregate list of identified consumers based on payment transactions for medical products or services.

⁷ 15 U.S.C. § 1681b(a), (g) state in relevant part:

(g) Protection of medical information

(1) Limitation on consumer reporting agencies

A consumer reporting agency shall not furnish for employment purposes, or in connection with a credit or insurance transaction, a consumer report that contains medical information (other than medical contact information treated in the manner required under section 605(a)(6) of this title) about a consumer

⁸ 15 U.S.C. § 1681c(a)(6) states in relevant part:

(a) Information excluded from consumer reports

Except as authorized under subsection (b) of this section, no consumer reporting agency may make any consumer report containing any of the following items of information:

* * * *

failure to safeguard her personal information and timely notify her of the Data Breach, her identity would not have been exposed, stolen and misused, nor would she have suffered “additional economic damages and other actual harm.” She seeks injunctive relief as well as statutory damages for these injuries.

A. Article III Standing

Article III of the Constitution limits the jurisdiction of federal courts to actual “Cases” and “Controversies.” U.S. CONST. art. III, § 2. “‘One element of the case-or-controversy requirement’ is that plaintiffs ‘must establish that they have standing to sue.’” *Clapper*, 133 S. Ct. at 1146 (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997)). “The doctrine of standing asks ‘whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.’” *Cibolo Waste, Inc. v. City of San Antonio*, 718 F.3d 469, 473 (5th Cir. 2013) (quoting *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 11 (2004)). Every party that comes before a federal court bears the burden of establishing the existence of an injury that is “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.” *Clapper*, 133 S. Ct. at 1147 (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)) (internal quotation marks omitted); accord *Cibolo Waste*, 718 F.3d at 473.

Regarding the first prong, the Supreme Court has repeatedly stated that “[a]lthough imminence is . . . a somewhat elastic concept,” it is not so elastic that it reaches allegations of “possible future injury.” *Clapper*, 133 S. Ct. at 1147 (emphasis in original; citations and internal quotation marks omitted). “An allegation of future injury may suffice if the threatened injury is

(6) The name, address, and telephone number of any medical information furnisher that has notified the agency of its status

‘certainly impending,’ or there is a ‘substantial risk’ that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (citing *Clapper*, 133 S. Ct. at 1147, 1150 n.5) (internal quotation marks omitted).

The second prong requires a “causal connection between the injury and the conduct complained of—in other words, the injury must be traceable to the defendant and not the result of the independent action of a third party.” *S. Christian Leadership Conference v. Supreme Court of State of La.*, 252 F.3d 781, 788 (5th Cir. 2001) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, [560–61] (1992)); see *Clapper*, 133 S. Ct. at 1150 (“We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.”). Finally, the third prong turns on the likelihood, as opposed to the mere speculation, that a favorable decision will redress the alleged injury. *S. Christian Leadership Conference*, 252 F.3d at 788 (citing *Lujan*, 504 U.S. [at 560–61]).

B. Imminent Injury

Peters argues that the increased risk she faces of future identity theft/fraud constitutes “imminent” injury. The Court cannot agree that she faces a “certainly impending” or “substantial” risk of identity theft/fraud as Article III requires, and her Complaint makes the point all too clearly. There, she cites reports from the GAO and FTC to lend credibility to her fear that savvy thieves could potentially use her personal information to: drain her bank account(s); make charges on her credit card(s) or on new cards fraudulently opened in her name; obtain false identification cards; perpetrate tax, medical and insurance fraud; or develop phishing schemes over the internet. Peters further raises the possibility that fraudulent use of her personal information could go undetected for long periods of time—even “years into the future”—and thus cause “significant harm to [her] credit rating and finances.”

“Unless and until these conjectures come true,” *Reilly*, 644 F.3d at 42, Peters’ alleged future injuries are speculative—even hypothetical—but certainly not imminent. Critically, Peters “cannot describe how [she] will be injured without beginning the explanation with the word ‘if.’” *Id.* at 43 (quoting *Storino v. Borough of Point Pleasant Beach*, 322 F.3d 293, 298 (3d Cir. 2003)) (internal quotation marks omitted). For example, Peters might be able to demonstrate harm *if* third parties become aware of her exposed information and reveal their interest in it; *if* they form an intent to misuse her information; and *if* they take steps to acquire and actually use her information to her detriment. The misuse of her information could take any number of forms, at any point in time. The risk of future harm is, no doubt, indefinite. It may even be impossible to determine whether the misused information was obtained from exposure caused by the Data Breach or from some other source. Ultimately, Peters’ theory of standing “relies on a highly attenuated chain of possibilities.” *Clapper*, 133 S. Ct. at 1148. As such, it fails to satisfy the requirement that “threatened injury be certainly impending to constitute injury in fact.” *Id.* at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

The future injuries alleged in this case fail for the same reasons the injuries in *Lujan* and *Clapper* were rejected by the Supreme Court. In *Lujan*, the plaintiffs, environmental conservationist organizations, sought to enjoin the funding of government activities that threatened the habitats of certain animal species. The Court held that standing could not be established based on the plaintiffs’ profession that they intended, “some day,” to visit project sites that would be impacted by these activities. *Lujan*, 504 U.S. at 564 & n.2. “Such ‘some day’ intentions—without any description of concrete plans, or indeed even any specification of *when* the some day will be—do not support a finding of the ‘actual or imminent’ injury that our cases require.” *Id.* at 564 (emphasis in original).

In *Clapper*, the Court addressed whether attorneys and human rights, labor, legal and media organizations had standing to challenge a provision of the Foreign Intelligence Surveillance Act of 1978 (“FISA”). The provision authorized the Government to acquire foreign intelligence information from communications of non-U.S. persons located abroad. The plaintiffs claimed that they faced harm stemming from a reasonable fear that persons with whom they exchanged foreign intelligence information—i.e., colleagues, clients, sources, and other individuals located abroad—would be likely targets of FISA-sanctioned surveillance. They alleged that the challenged provision would compromise their ability to “locate witnesses, cultivate resources, obtain information, and communicate confidential information to their clients.” *Clapper*, 133 S. Ct. at 1145. Furthermore, the threat of surveillance would compel them to take costly and burdensome measures to maintain the confidentiality of sensitive communications.

The plaintiffs asserted that “there [was] an objectively reasonable likelihood that their communication with their foreign contacts will be intercepted under [FISA] at some point in the future.” *Id.* at 1147. The Second Circuit accepted the argument, but the Supreme Court rejected it. The Court determined that the “objectively reasonable likelihood” standard was “inconsistent” with the long-standing requirement that threatened injury must be “certainly impending” to satisfy Article III. *Id.* at 1147-48 (citing cases).

Under *Clapper*, Peters must at least plausibly establish a “certainly impending” or “substantial” risk that she will be victimized. The allegation that risk has been increased does not transform that assertion into a cognizable injury. In fact, as one district court has observed, “*Clapper* seems rather plainly to reject the premise . . . that any marginal increase in risk is

sufficient to confer standing.” *Strautins v. Trustware Holdings, Inc.*, 27 F.Supp.3d 871, 878 (N.D. Ill. 2014).

It is worth noting that the Court also held that the alleged injuries were not fairly traceable to the challenged provision. In this regard, the Court rejected the argument that the plaintiffs were “suffering *present* injury because the risk of . . . surveillance already ha[d] forced them to take costly and burdensome measures to protect the confidentiality of their international communications.” *Clapper*, 133 S. Ct. at 1143 (emphasis in original); *see also Reilly*, 664 F.3d at 46 (“[C]osts incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more ‘actual’ injuries than the alleged ‘increased risk of injury’ which forms the basis for Appellants’ claims.”). *Contra In re Adobe Systems, Inc. Privacy Litig.*, No. 13-CV-05226-LHK, ---F.Supp.2d---, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014) (standing conferred where plaintiffs alleged they incurred expense to mitigate risk of increased risk of criminal fraud resulting from data breach); *Zappos.com*, 2013 WL 4830497 (same). The Court reasoned that standing cannot be “manufacture[d]” by the plaintiffs’ choice to inflict harm on themselves by making expenditures based on “hypothetical future harm.” *Clapper*, 133 S. Ct. at 1143, 1150–51. Otherwise, the Court cautioned, “an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.” *Id.* at 1151. Peters would therefore still fall short of the constitutional standard if she asserted any money spent prophylactically on credit monitoring services to “ease fears of future third-party criminality.” *Reilly*, 664 F.3d at 46.

The Court recognizes that before *Clapper*, a split existed among the Third, Seventh and Ninth circuit courts over whether the increased risk of harm stemming from a data security breach constitutes imminent injury under Article III. The Seventh and Ninth Circuits held that

such a risk was sufficient to confer standing. *Krottner*, 628 F.3d 1139; *Pisciotta*, 499 F.3d 629.⁹ The Third Circuit held that the risk fails the constitutional test. *Reilly*, 664 F.3d at 42-45. These decisions pre-date the two most recent Supreme Court cases that analyze Article III standing principles, however. *Susan B. Anthony List*, 134 S. Ct. 2334; *Clapper*, 133 S. Ct. 1138.

Arguably, *Clapper* has resolved the circuit split.¹⁰ Its holding compels the conclusion that Peters lacks standing to bring her federal claims to the extent they are premised on the heightened risk of future identity theft/fraud.

⁹ To reach its conclusion in *Pisciotta*, the Seventh Circuit drew analogies from Second, Fourth, Sixth and Ninth Circuit cases addressing defective medical device, toxic substance and environmental injury claims. *Pisciotta*, 499 F.3d at 634 n.3. The Court is not persuaded by *Pisciotta*'s reasoning. The Third Circuit cogently distinguished medical device and toxic substance claims, which "involve[] human suffering or premature death," from data breach claims, which do not. *Reilly*, 664 F.3d at 45. The critical standing question in these personal injury cases is not *if* damage has occurred, but rather *how* it will manifest. *Id.* In distinguishing environmental injury cases, the court observed that while a monetary award tends to restore data breach victims to their original position, money may not adequately remedy the harms suffered by environmental injury victims—e.g., the extinction of a species, the destruction of a habitat, or the polluting of air and water. *Id.* (citing *Cent. Delta Water Agency v. United States*, 306 F.3d 938 (9th Cir. 2002)). The court concurs that these distinctions place medical device, toxic substance and environmental injury victims in a separate category from data breach victims.

¹⁰ The Court notes that since *Clapper*, intra-circuit splits have developed among district courts in the Seventh and Ninth Circuits. In the Seventh Circuit, at least two courts have ruled that *Clapper* abrogated *Pisciotta* while one court disagrees. Compare *Strautins*, 27 F.Supp.3d 871 (Tharp, J.) ("*Clapper* compels rejection of [the plaintiff's] claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement of standing."), and *Barnes & Noble Pin Pad*, 2013 WL 4759588, at *3 (Darrah, J.) (citing *Clapper* to support proposition that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing), with *Moyer*, 2014 WL 3511500, at *5 (Bucklo, J.) ("I respectfully disagree with my colleagues that *Clapper* should be read to overrule *Pisciotta*'s holding . . .").

In the Ninth Circuit, one district court has determined that "the possibility of future harm is insufficient to establish standing." *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113-JSW, 2013 WL 1282980, at *5 (N.D. Cal. Mar. 26, 2013) (White, J.) (citing *Clapper*). That court distinguished *Krottner* from the facts before it and did not address whether *Krottner* and *Clapper* are reconcilable. At least three other district courts have concluded that *Krottner* was not affected by *Clapper*. E.g., *Adobe Systems*, 2014 WL 4379916 (Koh, J.); *Sony Gaming Networks*, 996 F.Supp.2d 942 (Battaglia, J.); *Zappos.com*, 2013 WL 4830497 (Jones, J.).

Other courts that have applied *Clapper* in the data breach context include district courts in the District of Columbia, the Southern District of Ohio, and the District of New Jersey. These courts have rejected the "increased risk" theory of standing. See *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, MDL No. 2360, ---F.Supp.2d---, 2014 WL 1858458 (D.D.C. May 9, 2014) (Boasberg, J.); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F.Supp.2d 646 (S.D. Ohio 2014) (Watson, J.); *Polanco v. Omnicell, Inc.*, 988 F.Supp.2d 451 (D.N.J. 2013) (Hillman, J.).

C. Actual Injury

The incidents identified by Peters as evidence of actual identity theft/fraud fail to meet the causation and redressability elements of the standing test. Peters essentially argues that her injuries are traceable to the FCRA because they stem from St. Joseph's failure to comply with the requirements of the statute. She contends that as a result of this failure, acts of identity theft/fraud were (and continue to be) perpetrated against her, albeit by *unknown third parties*, for which St. Joseph should be held responsible: the attempted charge to her credit card; the attempted access to her Amazon.com account; the telephone solicitations she has received from medical products and services companies; the spam email sent from her account; and the physical and electronic materials she has received targeting her recorded medical conditions.

Although it is alleged that St. Joseph's failures "proximately caused" these injuries, the allegation is conclusory and fails to account for the sufficient break in causation caused by opportunistic third parties. The injuries, to the extent that they meet the first prong, are "the result of the independent action of a third party" and therefore not cognizable under Article III. *S. Christian Leadership Conference*, 252 F.3d at 788 (citing *Lujan*, 504 U.S. [at 560-61]).

Even if the above injuries were traceable to St. Joseph's alleged failures under the FCRA, it is not likely that a favorable decision from this Court would redress the harm she has experienced. St. Joseph argues that Peters has not alleged any quantifiable damage or loss she has suffered as a result of the Data Breach. The Court agrees.¹¹

Moreover, some of Peters' injuries have already been remedied. Discover never charged her for the fraudulent purchase identified in the Complaint and closed her account to prevent

¹¹ The court notes that St. Joseph also cites as a pleading defect Peters' failure to allege any "unreimbursed cost" she incurred in mitigation of the Data Breach. The observation implies that such an allegation would meet the injury test. As discussed in Part V.B., voluntary mitigation expenses are not valid Article III injuries. *Clapper*, 133 S. Ct. at 1143, 1150-51.

future fraud. Upon discovery that her Yahoo email account had been compromised, Peters changed her password. The Complaint contains no allegations that her email contacts continue to receive voluminous spam email from her account since she took this proactive measure.

Finally, a ruling from the Court would not prevent medical products and services companies from contacting Peters or otherwise disgorge them of her personal information. Certainly, the Court can neither “control [n]or . . . predict” the “unfettered choices” made by these companies, who are not before the Court and are independent of St. Joseph in any event. *Lujan*, 504 U.S. at 562 (quoting *ASARO Inc. v. Kadish*, 490 U.S. 605, 615 (1989) (opinion of Kennedy, J.)).

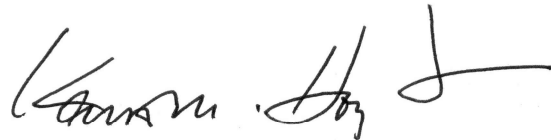
Peters has not made the requisite demonstration of injury, traceability and redressability for her alleged injuries. Lacking viability, her federal claims are dismissed with prejudice.

VI. CONCLUSION

Based on the foregoing analysis and discussion, the Court GRANTS St. Joseph’s Rule 12(b)(1) motion to dismiss for want of subject matter (federal question) jurisdiction and dismisses the Complaint without leave to amend. The Court expresses no opinion about the viability of Peters’ state or common law claims, however. Accordingly, the Court dismisses those claims *without* prejudice and GRANTS Peters 30 days to raise her remaining claims in state court.

It is so **ORDERED**.

SIGNED on this 11th day of February, 2015.

A handwritten signature in black ink, appearing to read "Kenneth M. Hoyt", written over a horizontal line.

Kenneth M. Hoyt
United States District Judge